

ABSTRACT OF THE DISCLOSURE

In each stage, multiple parallel nonlinear transformation modules each perform local lower-level diffusion, then a diffusion module performs higher-level diffusion over the block width and multiple parallel nonlinear transformation modules each perform local lower-level diffusion. This operation is repeated a predetermined number of times corresponding to the number of stages. Each nonlinear transformation module is formed into the nested SPN structure by arranging alternately nonlinear transformation modules and a diffusion module. The diffusion module performs linear transformation for spreading the state of at least one bit in input data to the preceding nonlinear transformation modules to at least one bit in input data to the succeeding nonlinear transformation modules.